

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

IN RE: DEALER MANAGEMENT SYSTEMS
ANTITRUST LITIGATION

MDL No. 2817
Case No. 18 C 864

This Document Relates to:
Authenticom, Inc. v. CDK Global, LLC, et al.,
Case No. 1:18-cv-00868 (N.D. Ill.)

Hon. Robert M. Dow, Jr.
Magistrate Judge Jeffrey T. Gilbert

PUBLIC-REDACTED

**AUTHENTICOM, INC.'S ANSWER AND AFFIRMATIVE AND ADDITIONAL
DEFENSES TO DEFENDANT CDK GLOBAL, LLC'S COUNTERCLAIMS**

INTRODUCTION*

1. CDK, Global LLC is one of the country's leading firms offering state-of-the art enterprise software known as dealer management systems ("DMS") and related services to Auto, Truck, Motorcycle, Marine, Recreational Vehicle, and Heavy Equipment dealerships. CDK's DMS offering (referred to herein as "CDK's DMS" or "the CDK DMS") primarily consists of two software products—Drive and DASH—that provide dealers with proprietary software tools and resources necessary to manage core aspects of their business. CDK's DMS currently is licensed to more than 27,000 dealerships across the world and more than 8,000 new and used car dealerships in North America.

ANSWER: Authenticom, Inc. ("Authenticom") admits that CDK Global, LLC ("CDK") is the country's largest provider of enterprise software known as dealer management systems ("DMS") and related services for franchised automobile dealerships. Authenticom admits that CDK's DMS provides franchised dealerships with software tools and resources they use to manage core aspects of their business. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations that relate to how many or the types of dealerships that use CDK's

* To the extent the headings or other content in the Counterclaims not contained in numbered paragraphs, such as section headings, are considered allegations within the pleading, Authenticom denies them.

products and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 1.

2 CDK's DMS also operates as an element of a larger automotive data "ecosystem" inhabited by dealers and other industry participants, including original equipment manufacturers ("OEMs") like General Motors, Ford, Toyota, Subaru, Porsche, and Jaguar; third-party software vendors that offer applications and solutions to dealers and OEMs; and CDK itself. Central to this automotive data ecosystem is CDK's DMS, which provides the infrastructure and intellectual property necessary for the ecosystem to securely and efficiently function.

ANSWER: Authenticom admits that CDK's DMS interacts with other industry participants including OEMs, third-party software vendors that offer applications, and CDK itself. Authenticom denies the remaining allegations in Paragraph 2.

3 One of the ways that CDK maintains the stability and security of its DMS is by requiring that third parties—for example, software application providers that wish to interact with the DMS—access the CDK DMS primarily through an approved interface known as "3PA."¹ The 3PA interface ensures that third parties only access the data they are properly authorized to access, and in a manner that is centrally managed by CDK in order to optimize data and system security and to prevent degradation of system performance and data corruption. As a means of enforcing this requirement, CDK dealers are contractually prohibited from giving unauthorized third parties access to the CDK DMS, including by giving those third parties login credentials meant for use solely by dealership employees.

ANSWER: Paragraph 3 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that the 3PA interface is necessary to ensure system data and system security; on the contrary, dealer-permissioned third-party access is consistent with a secure and stable system, as CDK itself recognized for many years prior to 2015. Authenticom denies the remaining allegations in Paragraph 3.

4 This limitation on third-party access is a feature of the CDK DMS that CDK believes is necessary to create and maintain a superior, better-functioning product. CDK dealerships, through their access to CDK's DMS, have access to myriad, highly-sensitive, commercially valuable data belonging to end-use customers (*e.g.*, the car-buying public), OEMs, and CDK itself. As data privacy and data misuse issues have markedly increased over the last several years (*e.g.*, Target and Sony, to name just a few), CDK has increased the number of security measures and system protections in place to protect all of this data and ensure that its customers

¹ More recently, the 3PA or "Third Party Access" program became known as the CDK Global Partner Program. For convenience, CDK will continue to refer to it as the 3PA program herein.

have a stable, secure, and multi-functional system to use in the efficient operation of their dealerships.

ANSWER: Denied.

5. One entity who *does not* benefit from CDK's exercise of control over its own proprietary software is counter-defendant Authenticom, whose business model is built around unrestricted (and uncompensated) access to CDK's DMS on behalf of software vendors and other third parties. Authenticom gains access to the CDK DMS by soliciting log-in credentials from dealers and essentially impersonating them. Authenticom then extracts data—not limited to data input by the dealers themselves—through a process known as “screen-scraping” and then *sells* that data to the vendors in exchange for a fee, often first copying the data into its own mirrored database called “DealerVault.” To make matters worse, for some vendors Authenticom also attempts, sometimes successfully, to “write back” *altered* data into the CDK DMS.

ANSWER: Paragraph 5 of the Counterclaims states legal conclusions and makes legal arguments to which no answer is required. To the extent an answer is required, Authenticom admits that it retrieves dealer data from the CDK DMS on behalf of, and with the permission and authorization of, the dealerships that own the data at issue, using a process that CDK publicly and repeatedly sanctioned. Authenticom denies the remaining allegations and characterizations in Paragraph 5.

6. All of this occurs outside of CDK's managed 3PA interface, meaning that so long as Authenticom has access to CDK's system, CDK has no way to control Authenticom's screen-scraping methods or prevent it from causing a data breach, degrading system performance, or corrupting files in the CDK DMS.

ANSWER: Authenticom admits that it does not participate in CDK's 3PA program today. Authenticom denies the remaining allegations in Paragraph 6.

7. Authenticom knows full well that its business model and conduct constitutes a flagrant breach of CDK's contracts with its dealers and an improper circumvention of CDK's DMS access restrictions, but Authenticom has refused for years to change its conduct, claiming that its activities are justified because dealers have “authorized” its unlawful conduct.

ANSWER: Paragraph 7 of the Counterclaims states legal conclusions and makes legal argument to which no answer is required. To the extent an answer is required, denied.

8. That position is mistaken. CDK's contracts with dealers (known as a Master Services Agreement or “MSA”) are clear that dealers are licensees of CDK's DMS and cannot

“authorize” or otherwise grant Authenticom or any other third parties any rights to access the DMS—certainly not over CDK’s express objections, which are presented to Authenticom each and every time it logs into the DMS. And even if dealers *could* give Authenticom access to just their own data in the CDK DMS, Authenticom accesses not only dealer data but also a significant amount of data (including OEM data and customers’ personal data and information) that does *not* belong to dealers. Such misappropriation of highly sensitive information that CDK is contractually bound to protect is not privileged by any reasonable measure.

ANSWER: Paragraph 8 of the Counterclaims states legal conclusions and makes legal argument to which no answer is required. To the extent an answer is required, denied.

9. Authenticom also attempts to justify its conduct by claiming that dealers’ only means of accessing data in CDK’s DMS is by allowing Authenticom to hack into the DMS and scrape it out for them. That is false. There are several other ways that dealers can access and share data with third parties, including through the use of reporting tools that CDK makes available to dealers. In fact, some CDK dealerships elect to gather data themselves using these tools so that vendors and other third-parties have no need to access the DMS at all.

ANSWER: Denied.

10. Although Authenticom paints itself as the victim—claiming the antitrust laws *require* CDK to allow it to pursue its parasitic practices—it is Authenticom’s conduct that is unlawful under a host of federal and state laws prohibiting unauthorized access to computers and unauthorized access to trade secrets and it is Authenticom’s cyber piracy that must be stopped. The Court should award CDK statutory and common law damages to compensate it for the costs of preventing Authenticom’s access to its DMS as well as equitable relief requiring Authenticom to permanently cease and desist its unauthorized DMS access and to disgorge the ill-gotten gains it has reaped from free-riding on CDK’s intellectual property and investments.

ANSWER: Paragraph 10 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, denied.

PARTIES

11. Counter-Plaintiff CDK Global, LLC is a Delaware limited liability company with its corporate headquarters and principal place of business at 1950 Hassell Road, Hoffman Estates, Illinois 60169. CDK is the largest global provider of integrated information technology and digital marketing solutions to the automotive retail industry, with more than 40 years of experience. CDK currently provides integrated technology solutions to over 27,000 Auto, Truck, Motorcycle, Marine, Recreational Vehicle and Heavy Equipment dealers throughout the world, including more than 8,000 new and used car auto dealers in the United States.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 11 of the Counterclaims and on that basis denies them.

12. The automotive data ecosystem that CDK supports is massive, with tens of thousands of installations of approved vendor applications and millions of transactions every day, supporting billions of dollars in commerce each year. CDK has made tremendous investments to build out and support its network of products and service offerings. Over the last three years alone, CDK has spent more than \$480 million researching, developing, and deploying new and enhanced product solutions for its customers.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 12 of the Counterclaims and on that basis denies them.

13. In light of its network's size, scope, and importance to the American economy, CDK has been designated by the Department of Homeland Security as a Critical National Infrastructure "so vital to the United States that [its] incapacitation would have a debilitating effect on security [and] national economic security."²

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 13 of the Counterclaims and on that basis denies them.

14. Counter-defendant Authenticom, Inc., is a privately held Wisconsin corporation with its corporate headquarters and principal place of business at 400 Main Street, La Crosse, Wisconsin 54601. *Authenticom* Complaint (*Authenticom* Dkt. 4) ("Compl.") ¶ 19.

ANSWER: Admitted.

NATURE OF THE COUNTERCLAIMS

15. These counterclaims arise under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201; the Defend Trade Secrets Act, 18 U.S.C. § 1836; the Wisconsin Computer Crimes Act ("WCCA"), Wis. Stat. § 943.70(2)(a); the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502; the California Unfair Competition Law, Cal. Bus. and Prof. Code § 17200; the Wisconsin Uniform Trade Secrets Act, Wis. Stat. § 134.90; and common-law theories of tortious interference, trespass to chattels, conversion, unjust enrichment, and fraud.

ANSWER: The allegations in Paragraph 15 of the Counterclaims state legal conclusions to which no response is required. Defendant's common-law conversion claim was dismissed under Federal Rule of Civil Procedure 12(b)(6); accordingly, no response is required as to that claim. Dkt. 506.

16. This Court has subject matter jurisdiction over these counterclaims pursuant to 28 §§ 1331, 1332(a)(1), and 1367(a). There is diversity jurisdiction under 28 U.S.C. § 1332(a)(1)

² See Dep't of Homeland Security, What is Critical Infrastructure?, *available at* perma.cc/N8JR-YQ6Y.

because CDK is a citizen of Illinois, Authenticom is a citizen of Wisconsin, and the amount in controversy with respect to these counterclaims exceeds the sum or value of \$75,000, exclusive of interest and costs. In addition, there is federal question jurisdiction under 28 U.S.C. § 1331 because CDK alleges violations of the CFAA, the DMCA, and the Defend Trade Secrets Act. There is supplemental jurisdiction over the state law counterclaims pursuant to 28 U.S.C. § 1367(a) because they are so related to CDK's federal-law counterclaims that they form part of the same case or controversy.

ANSWER: Authenticom admits that CDK is a citizen of Illinois and that Authenticom is a citizen of Wisconsin. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 16 of the Counterclaims that relate to the amount in controversy with respect to the counterclaims and on that basis denies them. The remaining allegations in Paragraph 16 state legal conclusions to which no response is required.

17. This Court has personal jurisdiction over Authenticom because it is located and does business in the District in which this action was filed; because many of the actions giving rise to these counterclaims occurred in, and/or were directed from, that District; and because Authenticom filed its complaint against CDK in that District.

ANSWER: The allegations in Paragraph 17 of the Counterclaims state legal conclusions to which no response is required. To the extent "that District" refers to the Northern District of Illinois, Authenticom denies that it filed its complaint against CDK in the Northern District of Illinois; on the contrary, Authenticom filed its complaint in the Western District of Wisconsin and any trial in this matter will take place in the Western District of Wisconsin. Authenticom likewise denies that "many of the actions" giving rise to CDK's counterclaims were "directed from" the Northern District of Illinois.

18. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c).

ANSWER: The allegations in Paragraph 18 of the Counterclaims state legal conclusions to which no response is required.

FACTUAL ALLEGATIONS

A. CDK's DMS

19. CDK has invested hundreds of millions of dollars to develop the hardware and software components of its DMS. CDK's DMS also includes, and is largely comprised of, valuable pieces of intellectual property, including patented technologies and proprietary software elements and programs created by CDK, each of which are accessed each time a user logs into and uses the DMS. At all relevant times, and as CDK's contracts with dealers and third parties make clear, the DMS has remained the sole and exclusive property of CDK. Dealers who purchase DMS services from CDK are granted a personal, non-transferable, license to *use* CDK's DMS in accordance with the terms and conditions of their agreement with CDK. Authenticom does not have such a license.

ANSWER: The allegations in Paragraph 19 of the Counterclaims state legal conclusions to which no response is required. To the extent an answer is required, Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations that relate to CDK's investments and on that basis denies them. Authenticom denies the remaining claims in Paragraph 19.

20. CDK's DMS offering consists of software and hardware components residing at both the dealership ("dealership network") and at CDK's data centers ("CDK network").³ CDK uses state-of-the-art technology to secure the connections between the dealerships and the CDK network, including through specialized hardware at each dealership site. That hardware creates a "virtual private network" ("VPN") or "Leased-Line Multiprotocol Label Switching network" ("MPLS") between the dealership and the CDK network, which accepts direct communications only from computers on the corresponding dealership's network.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 20 of the Counterclaims that relate to the full scope and operational details of CDK's DMS product and on that basis denies them.

21. CDK's terminal program that runs on dealer computers is an original and independent work created and licensed by CDK. It consists of original and distinct elements including its source and object code; distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience.

ANSWER: The allegations in Paragraph 21 of the Counterclaims state legal conclusions to which no response is required. To the extent an answer is required, Authenticom lacks sufficient

³ In a few instances, the server side of the DMS system is located on a dealership's premises rather than offsite at a CDK data center.

knowledge or information to form a belief as to the truth of the allegations in Paragraph 21 of the Counterclaims that relate to the composition of CDK's "terminal program" and on the basis denies them.

22. In addition to its core functionalities, the CDK DMS stores voluminous amounts of financial and accounting information and highly sensitive data, including financial statements, accounting data, payroll information, sales figures, inventory, parts data, warranty information, appointment records, service and repair records, vehicle information, customer personal identifiable information, intellectual property, and other third-party data. CDK encrypts sensitive data in the DMS and appropriately expunges data regularly.

ANSWER: Authenticom admits that the CDK DMS includes a database of dealer data. Whether that information is "highly sensitive" is a vague and subjective legal characterization to which no answer is required. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations that relate to the remaining allegations, including CDK's encryption and expungement practices, and on that basis denies them.

23. Not all of this data "belongs" to the dealers who use CDK's DMS. Some data is proprietary to OEMs, such as prices and part numbers for replacement parts, labor rates, and rebate, incentive and warranty information. Other data in CDK's DMS is proprietary to third-party service providers, such as credit reporting bureaus like Equifax, Experian, and TransUnion. Still other data in the DMS is CDK's own proprietary data, including forms, accounting rules, tax tables, and proprietary tools and data compilations. While access to third-party proprietary information in the DMS is permitted for licensed DMS customers, CDK is prohibited from sharing much of this information with unlicensed third parties. And CDK generally does not share its own proprietary information in the DMS with any third parties in the absence of a valid license. Authenticom does not have such a license.

ANSWER: The allegations in Paragraph 23 of the Counterclaims state legal conclusions to which no response is required. To the extent an answer is required, Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 23 of the Counterclaims that relate to any non-dealer-data stored on the CDK DMS, and on that basis denies them. Authenticom denies any implication that dealerships do not own all of the data relevant to Authenticom's business and/or this lawsuit.

24. CDK's DMS is password-protected. To access the DMS, each dealership employee must authenticate using his or her individual login credentials.

ANSWER: Authenticom admits that the CDK DMS is password-protected. Authenticom denies the remaining allegations in Paragraph 24.

25. Typically, at least one employee at each dealership using CDK's DMS has "administrator" level access privileges. An employee of a dealership who has submitted testimony in this case compared administrator-level access to CDK's DMS to possessing "the keys to the kingdom." 06/27/2017 Tr. (*Authenticom* Dkt. 165) 2-A-9:10-11. Users with administrator-level privileges have the authority to create new accounts (and corresponding login credentials) for other dealership employees. They also have the ability to define the data and functions each employee may access within CDK's DMS by creating and assigning the employees different "roles." In other words, each user has access to the DMS that is commensurate with the access privileges assigned to his or her user ID.

ANSWER: Authenticom admits that the cited transcript includes the phrase "keys to the kingdom," but denies any further characterization of the testimony, as the transcript speaks for itself. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 25 of the Counterclaims that relate to the "typical[]" practices of CDK's DMS customers concerning administrator access or the features of CDK's DMS "administrator" level access privileges, and on that basis denies them.

26. Data maintained in CDK's DMS are used in four primary application areas: Accounting, F&I Sales, Parts, and Service. The user IDs that dealerships create for their employees can be configured to have general access to all four functions or just certain of them. User IDs can also be configured to run reports, data queries, and writeback commands using what is known as an English Statement processor ("ENG"). [REDACTED]

ANSWER: Authenticom lacks sufficient information or knowledge to form a belief as to the "primary" application areas with respect to data maintained on the CDK DMS. Authenticom denies that the user IDs that dealers provide to Authenticom are always configured in any particular way and denies that Authenticom [REDACTED]

B. CDK's 3PA Program

27. Introduced by CDK in 2000, the 3PA program is a managed interface created for software application providers and other third parties to access and integrate with CDK's DMS. For example, several third-party marketing websites generate sales leads on behalf of dealerships. Those websites interface with CDK's DMS through the 3PA program to access sales transaction data, which they use to validate vehicle sales based on their sales leads. This is but one example of hundreds of third-party applications that integrate with CDK's DMS.

ANSWER: Admitted.

28. CDK's 3PA program has grown considerably in terms of both its sophistication and its number of participants, and its membership continues to grow today. Currently, the 3PA program provides more than 300 participants offering more than 400 applications with DMS integration through predefined integration points ("PIPs") that allow each application to extract and/or write data to CDK's DMS in a defined and controlled manner. Each PIP is a custom configuration based on the specific needs of the application it serves through a collaborative process between CDK and the respective 3PA program participant.

ANSWER: Authenticom admits that CDK's 3PA program has grown since it was first introduced, particularly in the aftermath of CDK's coordination and collusion with Reynolds. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 28 of the Counterclaims – including whether the 3PA program has grown in "sophistication"; the number of participants and integration points in the 3PA program; and how the predefined integration points or PIPs are configured – and on that basis denies them.

29. Importantly, PIPs also prevent third-party applications from accessing the DMS directly. Instead, PIPs create an interface *between* third-party applications and the DMS, relaying each application's request for data extraction or writeback to the DMS itself, which fulfills the request, and communicating the response back to the application. This is essential to facilitating safe and secure third-party access to CDK's DMS.

ANSWER: Authenticom denies that PIPs are "essential" to "safe and secure third-party access to CDK's DMS." Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the remaining allegations in Paragraph 29 and on that basis denies them.

30. Further, the use of PIPs ensures that a third party's software can only access data maintained in the CDK DMS in a reliable, secure, and supportable manner that will safeguard the integrity of the data and of CDK's system as a whole. Among other things, PIPs limit the third party's access to precisely the data and permissions it needs (and as approved by CDK). They also

allow CDK to audit all aspects of third-party access, including which precise data elements in the DMS are being accessed and how frequently they are being accessed.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 30 of the Counterclaims and on that basis denies them.

31. In addition, a managed 3PA interface allows CDK to place limits on the number of simultaneous transactions between third parties and the DMS, which prevents outside queries from overwhelming the system. CDK is able to pool system resources to serve each party's request sequentially and in the most efficient manner. And CDK has the ability to communicate with third parties using 3PA to alert them to system performance issues and manage troubleshooting. The managed 3PA interface also allows CDK to take steps to ensure that updates to CDK's DMS software and scheduled system maintenance do not disrupt third-party integrations and the risk of data corruption is minimized.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 31 and on that basis denies them.

a. 3PA Certification Requirements

32. The 3PA certification process consists of four phases: Orientation and Planning; Development; Certification; and finally, Deployment. During the Orientation and Planning stage, CDK works with third-party application vendors to determine their integration requirements, including the scope, workflows, frequency of access, and required data elements. CDK then proposes (and the parties agree to) an integration plan, which includes specifications for PIPs and other details of the integration. In the Development stage, the vendor builds the components of its application that will interface with CDK's DMS. The vendor's requested integrations are then configured and rigorously tested in a special staging environment using a "test" dealer linked to a set of accounts on a server that contain sample DMS data. Vendors are expected to implement logging into their integration framework, including the complete request and response for each data extraction, writeback command, etc. Logging is used to both troubleshoot any issues created by the interface and validate the precise data elements that are being copied from and/or written back to the CDK DMS. At the Certification stage, these results are verified and a final version of the software that the vendor plans to deploy is tested once again. Only after these steps are successfully completed does the application enter Deployment, when the application's interface is actually released into production. Each step is designed by CDK to protect the security, integrity, and performance of its DMS.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 32 and on that basis denies them.

33. Each third party certified under 3PA enters into a written agreement with CDK, including a Statement of Work that describes the integration (including PIPs) called for by the integration plan. In addition, among other things, the agreement obligates the vendor to access CDK's system only through its approved interface. The vendor also agrees to work with CDK on

an ongoing basis to ensure that the integration remains healthy as both CDK's and the third party's software evolves. The agreement also imposes liability on the vendor for misuse of the system or the data and requires the vendor to obtain written consent from the dealer before accessing its DMS and to refrain from re-syndicating the data to unapproved third parties. Further, the agreement indemnifies CDK for the vendor's failure to comply with data collection, privacy, and other applicable laws and regulations.

ANSWER: Paragraph 33 of the Counterclaims states legal conclusions and subjective characterizations to which no answer is required. To the extent a further response is required, Authenticom admits that vendors in the 3PA program sign a contract with CDK. Authenticom otherwise lacks sufficient knowledge or information to form a belief as to the truth of the remaining allegations in Paragraph 33 and on that basis denies them.

34. CDK also charges third-party participants in the 3PA program fees for the integration services it provides. These fees allow CDK to recoup its investment in both the 3PA program and the DMS itself and compensate CDK for the value of its services and the intellectual property that makes data integration possible.

ANSWER: Authenticom admits CDK charges participants in the 3PA program fees for the integration services the 3PA program provides. Authenticom denies that the 3PA prices CDK charges to vendors are necessary to recoup investment costs or to compensate CDK for the value of its services and intellectual property.

35. Authenticom is not a member of the 3PA program. CDK has no plans to admit Authenticom to the 3PA program, as Authenticom's entire business model is premised on free and unrestricted access to CDK's DMS. As a general matter, Authenticom does not have CDK's permission or its authorization to access or use CDK's DMS, including on behalf of or for the purported benefit of dealers or vendors.⁴

ANSWER: Paragraph 35 of the Counterclaims states legal conclusions to which no answer is required. To the extent a further response is required, Authenticom admits that it is not currently a member of the 3PA program and has not been since 2013. Authenticom lacks knowledge to say

⁴ There are a few one-off circumstances where CDK tolerates Authenticom's access to its DMS with respect to specific dealerships as a result of legacy contractual arrangements entered into by certain CDK affiliates, which CDK is working to eliminate as its contractual restrictions permit. Authenticom's continued access to the DMS in these few, specific instances is not at issue here.

whether CDK has plans to admit Authenticom into the 3PA program. Authenticom denies that its business model is premised on “free and unrestricted access to CDK’s DMS.” As Judge Peterson explained at the *Authenticom* preliminary injunction hearing, dealers pay CDK enormous sums for the DMS, and the dealers authorize Authenticom to access the DMS on their behalf; there is therefore no “free” access by anyone. Authenticom further denies that, as a “general matter,” CDK has not given its permission for Authenticom to access the CDK DMS; on the contrary, CDK’s DMS contracts expressly permit dealers to authorize Authenticom’s access as their agent.

b. Alternatives To 3PA

36. While many dealers and vendors exchange data through the 3PA program, it is not the only way that data residing on CDK’s DMS can be exchanged. CDK’s flagship DMS product, Drive, includes several reporting tools that dealers can use to compile and export their operational data, which they can use or distribute to third parties—including third-party application providers and entities like Authenticom. Some of these are the same reporting tools that Authenticom uses when it accesses the DMS using dealer-issued user IDs—the difference being that an actual dealership employee does not call them up hundreds or thousands of times throughout the day and night to constantly query data. Additional, more sophisticated reporting tools are also available to Drive users on an add-on basis.

ANSWER: Authenticom admits that CDK’s DMS includes multiple data reporting tools. Authenticom admits it uses some of these tools when retrieving dealer data at the dealer’s request and with the dealer’s authorization. Authenticom admits that it “accesses the DMS using dealer-issued user IDs.” Authenticom denies that it “constantly” queries data “throughout the day and night.” Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the remaining allegations in Paragraph 36 – including whether there are unidentified additional “sophisticated reporting tools” available to dealers – and on that basis denies them.

37. CDK dealers can and do use these reporting tools to share data with third-party vendors, often instead of having those vendors access CDK’s DMS through the 3PA program. This approach is not only viable; it is specifically approved by the National Auto Dealers Association (“NADA”), which published a set of data security guidelines for dealers in 2014 suggesting that dealers should “consider implementing a strict data ‘push’ system for sharing data.” Defs. P.I. Ex. 16 (*Authenticom* Dkt. 106-16).

ANSWER: Authenticom admits that some dealers have used the reporting tools described in Paragraph 37 to share data with third-party vendors. Authenticom denies this approach is a “viable” alternative to automated data integration. Authenticom admits the quoted language from the National Auto Dealers Association says the words “consider implementing a strict data ‘push’ system for sharing data” and denies any further interpretation of the cited document, as it speaks for itself.

38. Upon information and belief, several CDK dealers elect to “push” data to Authenticom that they obtain themselves from the CDK DMS using the reporting tools described above. Authenticom accepts data from dealers in this manner.

ANSWER: Authenticom admits that it has accepted data from some dealers in the manner described in Paragraph 38, but otherwise denies the allegations.

39. In addition, other DMS providers permit third-party access to their systems (including by Authenticom) outside of a certification program and/or without requiring those third parties to pay integration fees. If some dealers prefer that system, they are free to switch DMS providers. Some dealers have switched; many others have stayed or switched to CDK since it began taking steps to prevent unauthorized third-party access to its DMS.

ANSWER: Paragraph 39 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom admits that other (non-CDK) DMS providers permit third-party access to their systems, as CDK itself did up until it colluded with Reynolds. Authenticom denies that dealers are “free” to switch DMS providers; on the contrary, dealers face significant contractual, operational, and informational barriers to switching. Authenticom admits that some of the 18,000 dealerships in the United States have switched DMS providers, including to and from CDK. The remaining allegations are denied.

C. Authenticom’s Illegal Business Model

40. Authenticom refers to itself as a “dealer data integration provider,” Compl. ¶ 2, but that is a fiction. Authenticom admits that it offers “no *actual* ‘integration’” with CDK’s DMS “in the traditional sense,” only “data access.” Compl. ¶ 54 n.4.

ANSWER: Denied.

41. Authenticom is a free rider. Its business model revolves around gaining free access to DMSs (including CDK's DMS), extracting and exporting the data from those DMSs, often copying it into its own system, and then selling the data to third parties—principally vendors that provide software applications to support the dealers' operations. Authenticom is able to do this by acquiring login credentials from CDK dealers—often through unsecured means—and then using those credentials to access and query CDK's DMS thousands of times per day via automated software “scripts” often installed on dealer-owned computers, bypassing software controls that CDK has put in place to prevent such access along the way.

ANSWER: Denied. As Judge Peterson explained at the *Authenticom* preliminary injunction hearing, dealers pay CDK enormous sums for the DMS, and the dealers authorize Authenticom to access the DMS on their behalf; there is therefore no “free riding” or “free” access by anyone. Authenticom denies that it “sells” data to third parties; rather, it extracts dealer data, with dealer permission and authorization, and provides that data to third-party vendors of the dealer's choosing, just as CDK and Reynolds do. Authenticom admits that it acquires login credentials from dealers (again as CDK's DMI subsidiary does) but denies that it does so through “unsecured means.” Authenticom denies that it queries a dealer's DMS thousands of times per day. Authenticom denies that it bypasses software controls.

42. Once Authenticom has collected data from CDK's DMS by its unauthorized and unlawful methods, it often exports the data to its own mirrored database known as “DealerVault.” From there, Authenticom sells access to the data—precisely what it takes from CDK for free—to other third-party vendors, purportedly with the consent or “authorization” of dealers. Ironically, Authenticom requires vendors who access the data through DealerVault to enter into agreements that strictly prohibit them, among other things, from “furnish[ing] to any third party any Data provided to Vendor by DealerVault without written authorization from DealerVault or the Dealership” and obligating the vendors to “protect all Data provided by DealerVault so as to preclude access by any third party.” Pl. P.I. Ex. 76 (*Authenticom* Dkt. 151-4) §§ 1.2 & 1.4. Authenticom provides no such commitments to CDK, via contract or otherwise, before accessing CDK's proprietary DMS and extracting data.

ANSWER: Paragraph 42 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom admits that it uploads dealer data to DealerVault, with the dealer's permission and pursuant to the dealer's control. Authenticom denies that it “sells” dealer data, for the reasons described earlier. Authenticom denies that “takes”

data “from CDK for free”; all the data that Authenticom extracts on behalf of dealers is owned by the *dealer*, not *CDK* (as CDK itself has repeatedly and publicly acknowledged). Authenticom admits that its contracts with vendors contain the quoted language, but denies CDK’s characterizations of those documents. Authenticom’s contracts speak for themselves. Authenticom denies the remaining allegations in Paragraph 42.

43. Of course, Authenticom does not permit automated third-party access and screen-scraping from *its own* system, and it strictly prohibits dealers from sharing *DealerVault* user IDs and passwords with anyone other than “the unique authorized User to whom such password is assigned.” Pl. P.I. Ex. 28 (*Authenticom* Dkt. 71-3) § 6.7. Authenticom thus prohibits the same sort of third-party access and data syndication for DealerVault that it employs to siphon, and profit from, data residing on CDK’s DMS.

ANSWER: Paragraph 43 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom admits that its terms of service contain the quoted language, but denies CDK’s characterizations of those documents. Authenticom’s contracts speak for themselves. Authenticom denies the remaining allegations in Paragraph 43.

44. When Authenticom accesses CDK’s DMS using dealer-issued login credentials from a computer running on the dealer’s network, Authenticom’s CEO Steve Cottrell admits that the intent is to “emulate” an ordinary dealership employee (whose access would be permitted under the dealer’s MSA). 06/26/2017 Tr. (*Authenticom* Dkt. 164) 1-A-108:15-19. However, despite these and other efforts to evade detection,

[REDACTED]

ANSWER: Authenticom states that Mr. Cottrell’s testimony speaks for itself. Authenticom denies that it undertook action to “evade detection.” Authenticom denies that it has ever used [REDACTED]. Authenticom uses valid login credentials created by dealers (who in turn have the contractual authority to designate Authenticom’s access as the dealer’s agent). Authenticom lacks sufficient information and knowledge to form a belief as to the truth of the allegation that

[REDACTED] Authenticom's dealer-authorized access to the DMS. Authenticom denies the remaining allegations in Paragraph 44.

a. Misappropriation Of Proprietary Information

45. Each and every time that Authenticom accesses CDK's DMS from a dealer computer, it uses valuable pieces of intellectual property, including patented technologies and original software elements and programs. Each and every time that Authenticom accesses the CDK DMS, it creates a copy of portions of the DMS program code in the computer's Random Access Memory, as well as copies of the original and distinctive page layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience.

ANSWER: Paragraph 45 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, denied.

46. In addition, Authenticom's screen-scraping queries regularly access files containing proprietary information that belongs to neither it nor the dealers it purports to serve.

[REDACTED]

ANSWER: Paragraph 46 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom admits that it regularly retrieves certain parts files at the request of the dealers who grant Authenticom permission and authorization to access to those files, but denies the legal conclusion and characterization that those files contain

[REDACTED]. Authenticom denies the remaining allegations in Paragraph 46.

47. Authenticom's unauthorized access to these files is rampant. For example, an investigation performed by CDK in June 2017 showed that in just the preceding 30 days,

[REDACTED]

ANSWER: Paragraph 47 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom denies it accesses files without authorization. Authenticom lacks sufficient knowledge or information to form a belief as to the

truth of the allegations in Paragraph 47 of the Counterclaims that relate to the statistics of file retrieval as measured by CDK, and on that basis denies them.

48. Even when Authenticom does not access proprietary data directly, often it accesses and copies data that were created using CDK and third-party proprietary forms and functions within the DMS. For example, dealers use CDK's proprietary programs to calculate the expected monthly payment for a financed car deal based on inputs like the sale price, the customer's down payment, and the term. All four data elements in this example—including the monthly payment calculated using CDK's proprietary dataset—are stored in the DMS files that Authenticom can access, scrape, and copy into its mirrored DealerVault database.

ANSWER: Paragraph 48 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom denies that a car payment calculator is proprietary. Authenticom denies that it accesses or "copies" any non-dealer-owned proprietary information. Authenticom otherwise lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 48 of the Counterclaims and on that basis denies them.

b. Burdens On System Performance

49. Authenticom's methods of accessing and extracting data place considerably more strain on CDK's DMS than approved third-party access through the 3PA interface or the ordinary dealership employees for whom user ID/password access was designed, degrading system performance and consuming valuable computing resources.

ANSWER: Denied.

50. Third-party application providers often seek to replicate a narrow subset of data in the CDK DMS in their own databases. For example, a vendor offering a service appointment scheduling application may need to maintain up-to-date sets of service and repair order data from the DMS of each dealer it serves. This normally requires priming the vendor's database with a full dataset once, when the vendor begins providing services, and then updating the vendor's dataset with changes on an ongoing basis. In the 3PA program, vendors work with CDK to develop efficient data queries that retrieve only new data, cutting down on extraction of duplicative records and conserving computing resources. Nearly half of the third-party data extractions that occur through the 3PA interface are minimized in this manner.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 50 of the Counterclaims relating to the practices of third-party vendors and CDK's 3PA program functionality and on that basis denies them.

51. Authenticom, however, does not update its vendors' datasets with only the new data that they need to stay current. Instead, it often pulls a complete set of data *every* time it accesses the CDK DMS, and runs its queries constantly in order to mimic the *bona fide* integration available to vendors through the 3PA program. Authenticom repeats this process throughout the day for hundreds of dealers, adding to the cost of the computing services that CDK must provide to each of them. [REDACTED]

ANSWER: Denied.

52. Among the many guidelines and requirements of the 3PA program, vendors are restricted in most cases from performing bulk extraction queries between 5:00 a.m. and 10:00p.m. The purpose of this restriction is to minimize system burden and performance degradation caused by third-party access during dealership business hours. [REDACTED]

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 52 of the Counterclaims relating to CDK's 3PA program and its operation – including the alleged “purpose” of the program guidelines and requirements – and on that basis denies them. [REDACTED]

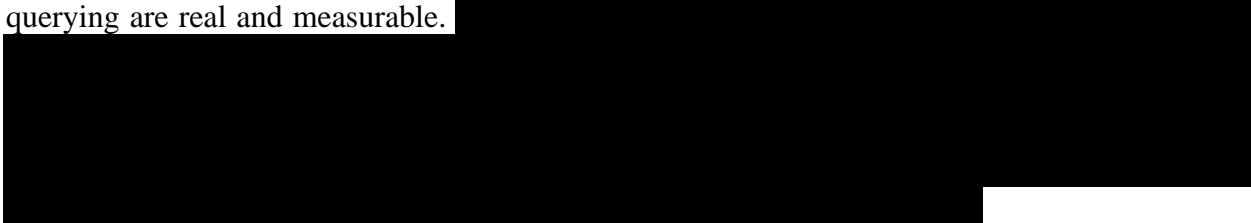
53. Investigations of Authenticom's data extraction methods show that Authenticom burdens CDK's systems with poorly-constructed, inefficient and repetitive queries that extract too much data, too frequently, and during peak dealer business hours. [REDACTED]

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to CDK's alleged analyses of Authenticom's data queries. Authenticom otherwise denies the allegations in Paragraph 53.

54. Because Authenticom hacks into the CDK DMS outside the 3PA interface and uses automated methods to extract data through decentralized interfaces that were designed for manual use by dealership employees, CDK effectively has no control over the queries that Authenticom runs or how frequently it runs them. CDK cannot manage the strain on system resources created by Authenticom or mitigate any performance issues that result.

ANSWER: Denied.

55. The burdens on CDK's DMS that result from Authenticom's constant access and querying are real and measurable.



ANSWER: Denied.

56. Authenticom has no incentive to minimize these burdens that it places on the CDK DMS: it didn't build the DMS, it doesn't pay for its operation or maintenance, and it doesn't deal with any issues that arise in its operation (and it doesn't have direct liability if the system fails). Instead, dealers who experience problems with the DMS call CDK—not Authenticom—and expect CDK to resolve the problem.

ANSWER: Denied.

c. Data Integrity Risks

57. An internal report prepared in 2013 by CDK's former parent company Automatic Data Processing, Inc. ("ADP") found that *all* of more than 2,900 CDK DMS servers examined had some level of data corruption issues, many of which were attributable to "hostile," unauthorized access to the DMS similar to Authenticom's methods of access.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the findings and accuracy of the report in Paragraph 57 and on that basis denies them. Authenticom denies any implication that the cited report attributed any "data corruption issues" to Authenticom; on the contrary, that report did not identify a single instance in which Authenticom caused a data corruption issue on the CDK DMS.

58. Moreover, in addition to extracting data from CDK's DMS, Authenticom also attempts to write back altered data to the DMS on behalf of at least some dealerships for whom it offers "data-cleansing" services. Cottrell Reply Decl. (*Authenticom* Dkt. 143) ¶ 46; *see also* Compl. ¶¶ 50, 54-55 & n.4, 77-80 (Authenticom seeks not only to "pull," "extract" and "scrape" data from CDK's DMS; but also to "push data back into the database" in altered form).

ANSWER: Authenticom admits that it sometimes writes back data on behalf of dealerships who request "data cleansing" services from Authenticom. Authenticom denies CDK's description of that data as being "altered."

59. Authenticom’s unauthorized “writeback” activity creates a high risk of introducing data errors and undermining the integrity of CDK’s DMS. CDK has formatting requirements called “business rules” for data fields in the DMS’s various databases, which govern precisely how applications should input data. When unauthorized third-parties attempt writeback functions, they often apply business rules incorrectly (or not at all) and cause data entry errors—which CDK is then responsible for fixing. While a manual error by a dealership employee can be a minor annoyance, a series of errors by automated systems—such as the scripts that Authenticom runs on CDK’s DMS—can rapidly propagate across an entire dataset, causing major disruption or denial of service. CDK can effectively address these risks for third- party application providers who access writeback functionality through the 3PA program through technical evaluations of the provider’s applications and extensive testing during the certification process. Pre-certification testing and evaluation also ensures that the application is not adversely affecting performance of the DMS. These sort of protections do not exist for Authenticom’s unauthorized, automated access using dealer-issued login credentials.

ANSWER: Denied.

d. Data Security Risks

60. Authenticom’s methods of accessing CDK’s DMS are significantly less secure than the 3PA managed interface that CDK requires approved third parties to use.

ANSWER: Denied.

61. As described above, 3PA participants access the CDK DMS through PIPs, which act as an intermediary between the participant’s application and the actual DMS. Before allowing any data to be transferred in or out of the DMS, the application must pass rigorous authentication protocols initiated by the PIP. The authentication token that each application uses is transmitted through a secured communication channel. By contrast, Authenticom uses dealer- issued login credentials that it often obtains through unsecured channels, including plain-text email. This exposes the credentials—and by extension, CDK’s DMS—to the risk of interception or compromise and violates widely accepted cybersecurity practices.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 61 of the Counterclaims relating to 3PA participants and the 3PA application process. Authenticom admits that it uses dealer-issued login credentials but denies that it “often obtains credentials from dealers through unsecured channels, including plain-text email.” Authenticom denies the remainder of the allegations in Paragraph 61.

62. [REDACTED]

[REDACTED]

ANSWER: Denied.

63. Authenticom's use of dealer-issued login credentials is particularly concerning to the extent that Authenticom implemented a software tool, as it bragged to one CDK dealer, that automatically re-enables any disabled user IDs "every hour." Defs. P.I. Ex. 41 (*Authenticom* Dkt. 106-48). This software was run by an administrator-level account at the dealership—the highest level of user access permitted for CDK's DMS, usually limited to one or two trusted employees at each dealership.

[REDACTED]

ANSWER: Denied.


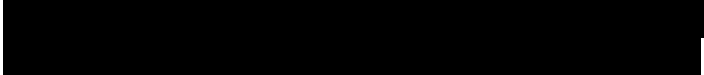
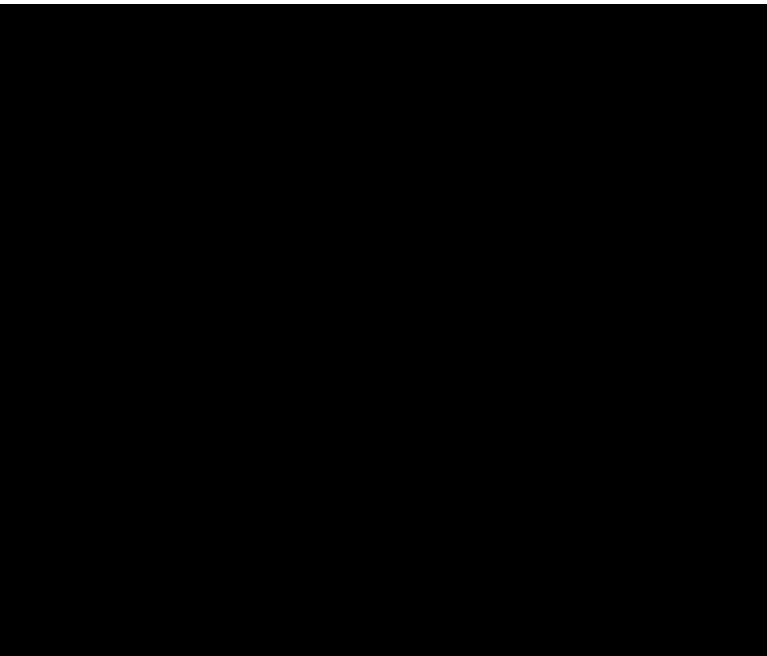
64. Authenticom's methods also violate the tenet of data minimization, *i.e.*, that each user of a secured system should receive no greater access or privileges than necessary. The 3PA interface abides by this principle and strictly controls each participant's access at a granular level, to only those specific data needed for that party's approved purposes. By contrast, Authenticom claims that "[a]s a matter of practice," it accesses and scrapes data from all primary directories in the CDK DMS for every dealer: sales, service, inventory, customers, and parts. Cottrell Reply Decl. ¶¶ 3, 13. What this means, and what CDK's investigation indicates, is that Authenticom's user IDs regularly have access to (and often, are constantly querying) all application areas in CDK's DMS, regardless of whether the purported end users—the application providers—actually need or have even asked for such access.

ANSWER: Authenticom denies the legal conclusion that its methods "violate the tenant of data minimization." Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 64 of the Counterclaims relating to CDK's own operations, including the details of the 3PA program, and on that basis denies them. To the extent the allegations in Paragraph 64 of the Counterclaims rely on or characterize documents outside the pleadings, Authenticom denies those allegations, as the documents speak for themselves. Authenticom denies that it "scrapes data from all primary directories in the CDK DMS for every

dealer”; denies that it is “constantly querying” all application areas in the CDK DMS; and denies the remaining allegations in Paragraph 64 of the Counterclaims.

65. Against this backdrop, Authenticom argues that CDK should simply trust that Authenticom is an honest data broker and that its data security practices are adequate. However, even if CDK could bear the risk of taking Authenticom at its word on these points (and it cannot), evidence directly contradicting these assurances have already emerged.

ANSWER: Denied.

66. For example, in August 2016, CDK implemented a security measure to disable numerous user IDs that Authenticom was using to perpetrate its unauthorized data scraping. In response, 



ANSWER: Authenticom admits that CDK took actions in August 2016 to disable many user IDs that dealers had created and issued to Authenticom. Authenticom denies that its activities were unauthorized, or that CDK’s actions can be characterized as “a security measure.” Authenticom states that the email excerpt pictured in Paragraph 66 was edited and altered by CDK and speaks for itself.

67. [REDACTED]

[REDACTED] Contrary to Mr. Cottrell's sworn testimony that "[i]t has been—and continues to be—Authenticom's policy that ... if a dealer prefers to send login credentials via email, that the username and password be sent to Authenticom in separate emails," Cottrell Reply Decl. ¶ 23, [REDACTED]

ANSWER: Authenticom admits that it sent emails to dealerships whose login credentials were blocked by CDK in August 2016. Authenticom denies that the content of the emails in question was "contrary" to Mr. Cottrell's testimony or Authenticom's policy. Authenticom states that Mr. Cottrell's testimony speaks for itself. The other allegations and characterizations are denied.

68. Authenticom's CEO Mr. Cottrell also falsely represented in both this litigation and to the marketplace that Authenticom had for three years received a Microsoft "gold security certification" with respect to its data extraction methods—a certification that does not, in fact, exist. *Compare* Cottrell Decl. (Authenticom Dkt. 62) ¶ 31 with 06/26/2017 Tr. (Authenticom Dkt. 162) at 1-P-25:15-26:10. In any event, Microsoft itself is clear that simply being a customer of its Azure storage platform does not ensure Authenticom is secure or obviate Authenticom's many security obligations.⁵ Indeed, a highly publicized recent data breach at Deloitte occurred on the same Microsoft Azure platform that Authenticom uses.⁶

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations that relate to the nonparty Deloitte and on that basis denies them. The remaining allegations are denied.

69. Mr. Cottrell further testified that DMSs are "not a high value target" for hackers. 06/26/2017 Tr. at 1-P-23:2-5. That statement is patently illogical, given the reams of sensitive personal and financial data that are maintained in DMSs, including CDK's DMS. Moreover, at least one DMS solution—offered by competitor DealerBuilt—has *already* suffered a serious data security breach resulting in millions of customers' confidential information being compromised. Defs. P.I. Ex. 151.⁷ Although the DealerBuilt data breach was widely reported, Mr. Cottrell testified that he remained unaware that the breach had even occurred for nearly ten months. 06/26/2017 Tr. at 1-P-22:1-6

⁵ See Frank Simorjay, *Shared Responsibilities for Cloud Computing* at 5 (Microsoft White Paper, April 2017), available at <https://perma.cc/3D2Q-TCPH>.

⁶ See, e.g., Nick Hopkins, Deloitte hit by cyber-attack revealing clients' secret emails, *The Guardian* (Sep. 25, 2017), available at <https://perma.cc/7PVL-3FS3>.

⁷ See also Zack Whittaker, Bought a Car Recently? Millions of dealership customer details found online, *ZDNet* (Nov. 8, 2016), available at <https://perma.cc/4K85-8GQN>.

ANSWER: Authenticom states that Mr. Cottrell’s testimony speaks for itself. Authenticom admits that DealerBuilt experienced a data breach – which was unrelated to third-party data integration – and otherwise denies Paragraph 69’s allegations and characterizations related to that incident. Authenticom denies the remaining allegations in Paragraph 69.

70. Authenticom also touts a purported \$20 million cybersecurity insurance policy, but that policy by its terms provides no coverage to CDK in the event of a data breach. Moreover, as just some examples, to settle their respective data breaches Home Depot reportedly paid out more than \$150 million⁸ and Target more than \$200 million.⁹ It is unrealistic to think that a \$20 million insurance policy could remedy the potential harm that would result from a breach of Authenticom’s DealerVault data warehouse.

ANSWER: Paragraph 70 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom admits that it has a \$20 million cybersecurity insurance policy. That policy speaks for itself. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 70 of the Counterclaims that relate to entities other than Authenticom, and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 70 of the Counterclaims.

D. CDK Prohibits Authenticom’s Unauthorized Access

a. Contractual Prohibitions

71. In order to protect against unauthorized access to the sensitive and proprietary data maintained in CDK’s DMS, the MSA between CDK and its dealer customers expressly prohibits dealers from supplying login credentials to third parties or otherwise granting third parties access to the DMS: “Client shall not allow access to [the CDK DMS] by any third parties except as otherwise permitted by this agreement.” MSA § 4(D). Dealers are also prohibited from causing or permitting “ANY THIRD PARTY SOFTWARE TO ACCESS THE [CDK DMS] EXCEPT AS OTHERWISE PERMITTED BY THIS AGREEMENT.” *Id.* § 4(B). Nowhere does the MSA permit access by Authenticom.

⁸ Jeff John Roberts, *Home Depot to Pay Banks \$25 Million in Data Breach Settlement*, Fortune Magazine (March 9, 2017), available at <https://perma.cc/H5A8-XAP6>.

⁹ Reuters, *Target Pays Millions to Settle State Data Breach Lawsuits*, Fortune Magazine (May 23, 2017), available at <https://perma.cc/PP9R-HQVA>.

ANSWER: Paragraph 71 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom denies CDK included the contractual provisions referred to in Paragraph 71 for security purposes. Authenticom states that CDK's DMS contract speaks for itself.

72. Pursuant to the MSA, the dealer expressly agrees, among other things, that it will only use CDK's software "for its own internal business purposes and will not sell or otherwise provide, directly or indirectly, any Products or Services, or any portion thereof to any third party" (*id.* § 4(B)); and that it will "treat as confidential and will not disclose or otherwise make available any of the Products or Services (including, without limitation, screen displays or user documentation) or any ... proprietary data, information, or documentation related thereto ... in any form, to any person other than employees of [the dealer]..." (*id.* § 4(D)). The dealer also acknowledges that notwithstanding its license to use the CDK DMS, the DMS remains at all times "the exclusive and confidential property of [CDK]." *Id.* § 4(A).

ANSWER: Paragraph 72 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom states that CDK's DMS contract speaks for itself.

73. Every version of CDK's standard MSA since at least 1994 has expressly stated that dealers are prohibited from permitting unauthorized third parties to access their licensed DMS. Further, the language quoted above has remained substantially the same in every version of the MSA since approximately 2010.¹⁰

ANSWER: Paragraph 73 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom denies that CDK's DMS contract has prohibited third parties to access the DMS; on the contrary, the CDK DMS contract expressly authorizes dealers to appoint third-party agents such as Authenticom to access the DMS on the dealer's behalf. Authenticom further states that CDK's DMS contract speaks for itself.

74. Authenticom is well aware that its business model and method of accessing CDK's DMS violates the express terms of the MSA between CDK and its dealer customers. Upon information and belief, Authenticom has been aware of this fact for *years*.

ANSWER: Denied.

¹⁰ Prior to 2017, the provisions quoted above appeared in Section 6 of the MSA; they now appear in Section 4.

75. A prior version of CDK's MSA prohibited dealers from making the DMS available "to any person other than employees and agents of [the dealer] with a need-to-know." Authenticom has recently begun asserting—once this litigation began—that its access to CDK's DMS was permitted under this language because Authenticom supposedly is the dealer's "agent." That assertion is directly contradicted by Authenticom's own Complaint, in which it attempted to assert an antitrust claim—which was dismissed by the Court—premised on a theory that the express restrictions on unauthorized third-party access in CDK's MSA constitute "exclusive dealing." *See* Compl. ¶¶ 150-56. Moreover, Authenticom's own contract with dealers makes clear that Authenticom is not the dealer's "agent," and in fact refers to "agents" of the dealer repeatedly as third parties to the agreement. Pl. P.I. Ex. 28 (*Authenticom* Dkt. 65-3) §§ 1.12, 3.2, 8.1, 104. Finally, even if an "agent" exception existed (and it does not), the MSA independently prohibits "ANY THIRD PARTY SOFTWARE TO ACCESS THE CDK DEALER MANAGEMENT SYSTEM." MSA § 6(B).

ANSWER: Paragraph 75 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom states that the CDK DMS contract and the other documents cited in Paragraph 75 speak for themselves. Authenticom otherwise denies the allegations in Paragraph 75.

b. CDK's Enforcement Of Its Third-Party Access Restrictions

76. At one time, notwithstanding the MSA's prohibition on unauthorized third-party access, CDK did not actively enforce these contract rights; it did not seek to prevent dealers from providing login credentials to third parties and did not actively take steps to block third parties from accessing the CDK DMS with these credentials. Events over the last decade, however, caused CDK to fundamentally change its approach to data security and third-party access. By March 2013, CDK was warning dealers to "[n]ever allow third parties to use your user ID or 'screen scrape' your data." Defs. P.I. Ex. 21 (*Authenticom* Dkt. 106-23).

ANSWER: Paragraph 76 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom admits that up until 2015, CDK did not prevent dealers from providing login credentials to third parties and did not actively take steps to block third parties from accessing the CDK DMS with these credentials. Authenticom denies that CDK changed its approach "over the last decade"; in fact, CDK changed its approach in 2015 – less than four years ago – and only after coordinating and colluding with Reynolds. Authenticom states that the document cited in Paragraph 76 speaks for itself. Authenticom denies the remaining allegations in Paragraph 76.

77. Moreover, beginning later that year and in 2014, a number of high-profile data security breaches across multiple industries cost US companies millions of dollars and put sensitive customer information for millions of people at risk:

- a) In November and December 2013, online thieves successfully hacked into the computer network at against Target, one of the largest retail companies in the United States. The hackers stole credit card or personal information from up to 70 million customers. Both personal data and credit card information may have been stolen from about 40 million people.
- b) In June 2014, North Korea conducted the first-ever destructive cyber attack against the United States when it launched destructive malware attacks against Sony Pictures Enterprise (“Sony”). In addition to destroying Sony data and systems, the attackers stole approximately 100 terabytes of sensitive company and employee data. The cyber attack led to the firing of Sony’s CEO.
- c) In August 2014, Community Health Systems, the largest provider of general hospital healthcare services in the United States, informed the Securities and Exchange Commission that hackers “originating from China” had stolen sensitive information on 4.5 million patients.
- d) In 2016, a security breach at competing DMS provider DealerBuilt exposed millions of customer records of personal and financial data, making them vulnerable to cybercrime and fraud.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 77 of the Counterclaims, all of which relate solely to entities that are not parties to this litigation, and on that basis denies them.

78. These well publicized data breaches brought new focus to the risks that CDK was taking by continuing to tolerate unchecked third-party access to its DMS.

ANSWER: Denied.

79. On September 30, 2014, CDK was officially spun off from ADP and began to operate as an independent, publicly-traded company. CDK’s executive leadership quickly realized that a lack of stringent security surrounding its DMS created an unacceptable liability risk for any publicly-traded company. The lack of such security was also allowing free-riders like Authenticom to profit off hundreds of millions of dollars in capital investments and intellectual property to which Authenticom had not contributed a dime.

ANSWER: Authenticom admits that CDK spun off from ADP in 2014. Authenticom denies that the spin-off was the impetus for CDK’s policy switch and eventual blocking of third-party

integrators, which occurred when CDK coordinated and colluded with Reynolds. Authenticom denies that is a “free rider” that has profited off CDK’s capital investments; on the contrary, dealers pay CDK enormous sums for DMS services, and Authenticom extracts dealer data on behalf of those dealers with their permission and authorization. There is therefore no free riding by anyone. Authenticom denies the remaining allegations in Paragraph 79.

80. In January 2015, CDK engaged PwC to conduct an assessment of its security program. PwC’s report concluded that CDK faced an “[i]ncreased risk exposure from not knowing or assessing all vendors that have access to CDK facilities, assets and data.” In consultations with CDK that followed, PwC specifically recommended that CDK secure its DMS to eliminate the security risks presented by unauthorized third-party access.

ANSWER: Authenticom admits that CDK engaged PwC to conduct an assessment. That document speaks for itself and Authenticom denies the allegations that purport to characterize it. Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations concerning purported conversations between PwC and CDK and on that basis denies them. Authenticom denies the remaining allegations in Paragraph 80.

81. In June 2015, CDK announced a multipart strategy called “SecurityFirst,” one aspect of which was an initiative by the company to remove third-party code installed on its DMS and eliminate unauthorized third-party access, including through the use of dealer-issued login credentials. When SecurityFirst was announced, over 52% of CDK’s DMS servers were infected with “hostile” code and 27,000 user IDs were being used by unauthorized third parties. A large number of those user IDs were attributable to Authenticom.

ANSWER: Authenticom admits that, in June 2015, CDK announced a strategy it marketed as “SecurityFirst.” Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 81 that relate to CDK’s internal operational details and investigations, and on that basis denies them. To the extent Paragraph 81 alleges that Authenticom ever placed “hostile code” on the CDK DMS, Authenticom denies that allegation. Authenticom denies the remaining allegations of Paragraph 81.

82. CDK's SecurityFirst announcement was well publicized within the industry. Upon information and belief, Authenticom became aware that CDK objected to its unauthorized access to the CDK DMS no later than June 2015, and in all likelihood, much earlier.

ANSWER: Paragraph 82 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom denies that it "became aware that CDK objected" to Authenticom's access by June 2015 (or any other date); on the contrary, CDK affirmatively authorized Authenticom's agent access through the CDK DMS contract. Authenticom denies that its dealer-permission data integration services are unauthorized.

c. Authenticom's Attempts To Evade CDK's Security Measures

83. In 2016, CDK began actively implementing security measures to prevent unauthorized access to its DMS by Authenticom and a number of other "hostile" third-party vendors and data extractors. At each step, Authenticom has constantly attempted—often successfully—to circumvent CDK's security measures, including by falsely certifying to CDK that it is an authorized DMS user.

ANSWER: Paragraph 83 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom denies that its operations were "unauthorized" or "hostile." Authenticom admits that CDK's blocking greatly disrupted Authenticom's business and client relationships. Authenticom denies that it "constantly attempted" to "circumvent" CDK security measures. Authenticom denies that it falsely certified it was an authorized DMS user.

84. For example, CDK created a log-in prompt, shown below, to address suspected unauthorized third-party access to its DMS. The prompt notified users that "[t]he CDK Global DMS is for authorized Dealer personnel only. Use or access by unauthorized third parties is prohibited. ... Enter 'YES' to confirm you are an authorized dealer employee in order to continue. Enter 'NO' to exit this program." In other words, users had to represent to CDK that they were "an authorized dealer employee" before they could access the CDK DMS:

```

login: heidi
Password:
Last login: Thu Mar 24 09:10:10 from 139.126.150.113
A RAID EVENT has been reported in the raid event directory.
It is important to notify your CRR of this RAID EVENT as soon as possible.
The CDK Global DMS is for authorized Dealer personnel only.
Use or access by unauthorized third parties is prohibited.
Those using this system without authorization will be denied
access and may have their services revoked.
Enter "YES" to confirm you are an authorized dealer employee
in order to continue, enter "NO" to exit this program.
yes

```

ANSWER: Authenticom states that to the extent the image (and description of that image) provided in Paragraph 84 is an allegation, the image speaks for itself. Authenticom denies the remaining allegations of Paragraph 84.

85. Between approximately March and July, 2016, this log-in prompt was deployed to more than [REDACTED] user IDs that Authenticom was using to access CDK's DMS. Each time, Authenticom modified its scripts to automatically enter "YES" in response to the log-in, thereby representing to CDK that the script was "an authorized dealer employee."

ANSWER: Paragraph 85 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 85 of the Counterclaims which relate to CDK's software, including the scope of the deployment of the log-in prompt, and on that basis denies them. Authenticom denies any implication that Authenticom lacked proper authorization to access dealer data stored on the CDK DMS on the dealer's behalf. The remaining allegations are denied.

86. Authenticom made these representations to CDK knowing that they were false, and for the purpose of tricking CDK's DMS into allowing Authenticom's scripts to access the system and scrape data. By altering its scripts to falsely certify that they were authorized dealer employees, Authenticom was able to regain access to CDK's DMS.

ANSWER: Paragraph 86 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, denied.

87. In April 2016, former CDK employee Dan McCray spoke with Authenticom's CEO Steve Cottrell in person while both happened to be attending the same industry conference and informed him (a) that CDK's contracts with dealers prohibited them from providing DMS

login credentials to third parties (including Authenticom) and (b) that CDK intended to prevent non-authorized access to its DMS, including Authenticom's unlawful user ID and password access. Mr. Cottrell responded to the effect that Authenticom refused to cease its unauthorized access or otherwise change its business practices.

ANSWER: Authenticom admits that Dan McCray and Steve Cottrell spoke in person while at an automotive industry conference in April 2016. Authenticom denies Paragraph 87's characterization and description of that conversation.

88. In approximately June 2016, CDK began requiring password changes for user IDs associated with unauthorized automated third-party access, including several hundred accounts being used by Authenticom. This was a security measure implemented by CDK to effectively disable any accounts that were not being used by authorized dealership employees (who would be capable of easily changing their password). Temporarily, this worked to block Authenticom's scripts from accessing the system. But within a matter of days, Authenticom modified its scripts once again to automatically change the passwords for each of the affected user IDs. By doing so, Authenticom was able to regain access to CDK's DMS.

ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations about the alleged June 2016 software change. Authenticom denies that the blocking of third-party integrators was a "security measure." Authenticom admits that it worked with dealers to reestablish dealer-created login credentials (as CDK did when Reynolds blocked DMI's dealer-permissioned access). Authenticom denies the remaining allegations of Paragraph 88.

89. The following month, CDK began permanently disabling certain user IDs that Authenticom was using to access the CDK's DMS. Authenticom claims that this effectively blocked its use of "thousands" of user IDs, at least temporarily. *See* Cottrell Decl. (Authenticom Dkt. 62) ¶ 39 ("CDK disabled Authenticom's login credentials, affecting thousands of dealership connections."); Compl. ¶ 189. However, as described in further detail above, Authenticom soon responded by soliciting dealers to create new user IDs and by offering to install software on the dealer's network that uses an administrator-level account to access the CDK's DMS and automatically re-enable all other disabled accounts "every hour."

ANSWER: Authenticom admits that CDK disabled certain user IDs that Authenticom was using. Authenticom states that the documents cited in Paragraph 89 speak for themselves. Authenticom admits that it worked with dealers to reestablish dealer-created login credentials (as

CDK did when Reynolds blocked DMI's dealer-permissioned access). Authenticom admits it offered a small number of dealers a script to empower dealers to re-enable disabled login credentials. The remaining allegations in this Paragraph are denied.

90. More recently, in November 2017, CDK also introduced a CAPTCHA control designed to stop Authenticom's automated access:



ANSWER: Authenticom lacks sufficient knowledge or information to form a belief as to the truth of the allegations in Paragraph 90, and on that basis denies them. Authenticom states that to the extent the image provided in Paragraph 90 is an allegation, the image speaks for itself.

91. The CAPTCHA could not be more clear that “[o]nly dealer personnel are authorized to use the CDK Global DMS. Use or access by unauthorized third parties is strictly prohibited and is in violation of the terms on which CDK licenses its software and services. Machine/automated access ... or issuing of user names and passwords for third party use is considered non-authorized access.” The CAPTCHA then requires the user to identify a word or

series of letters and numbers, as shown above, to “confirm you are an authorized dealer employee” before successfully logging into the CDK DMS.

ANSWER: Paragraph 91 of the Counterclaims states legal conclusions about the interpretation of CDK’s CAPTCHA prompt to which no answer is required. To the extent the allegations in Paragraph 91 seek to construe the image in Paragraph 90, Authenticom states the image speaks for itself.

92. Humans can easily pass CAPTCHA tests, but automated scripts—like the ones that Authenticom uses—often encounter difficulty. Accordingly, CDK deployed a CAPTCHA test to hundreds of specific user IDs associated with, among others, Authenticom in order to prevent its automated access to the CDK DMS. It worked, for a moment. However, Authenticom was able to crack the CAPTCHA almost immediately and regain access. CDK does not yet know exactly how Authenticom is circumventing the CAPTCHA. But in doing so, Authenticom once again falsely certifies to CDK that it is “an authorized dealer employee” in order to bypass a security measure specifically designed to keep it out of the system.

ANSWER: Paragraph 92 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom lacks sufficient knowledge or information as to why CDK deployed CAPTCHA and its efficacy. Authenticom denies that it “crack[ed]” or “circumvent[ed]” the CAPTCHA prompt. Authenticom denies that it falsely certifies itself as an authorized user; dealers specifically authorize Authenticom to access dealer data on their behalf, as CDK’s DMS contracts permit dealers to do. The remaining allegations in this Paragraph are denied.

93. Authenticom has been unmistakably clear that unless it is stopped once and for all, it will continue circumventing CDK’s security measures by any means available. [REDACTED]

[REDACTED] A few months later, in November 2016, Mr. Cottrell issued another letter touting that Authenticom had found “a technology solution” to CDK’s security measures—the profile re-enabling program described above—and was working to “deploy the solution across thousands of dealerships.” Defs. P.I. Ex. 44 (*Authenticom* Dkt. 106-51). Authenticom has further admitted during the course of discovery that it continues to use dealer-issued login credentials to access CDK’s DMS—in direct violation of CDK’s agreements with those dealers—and that it “works with affected dealers to reestablish ... connections” whenever CDK disables them, a statement that Authenticom echoes in its complaint. *See* Compl. ¶ 195 (Authenticom “work[s] cooperatively” with dealers to “set up new credentials and reestablish access”).

ANSWER: Paragraph 93 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom denies the allegations in the first sentence of Paragraph 93 of the Counterclaims. The documents quoted in Paragraph 93 speak for themselves. Authenticom denies the allegations purporting to characterize those documents or the statements in them. Authenticom denies it has admitted to using dealer-issued login credentials “in direct violation of CDK’s agreements with those dealers”; on the contrary, CDK’s DMS contract expressly permit dealers to authorize Authenticom to access the DMS as the dealer’s agent. Authenticom admits that it works with dealers to reenable dealer-issued login credentials (as CDK did when Reynolds disabled DMI’s login credentials).

94. Even today, more than two years after CDK began taking steps to eradicate illegal, hostile access to its DMS, Authenticom still accesses CDK DMS hundreds of times every day using new user IDs and passwords that it obtains. Even when CDK permanently disables those user IDs, new ones spring up just as quickly and resume querying and extracting data.

ANSWER: Paragraph 94 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom denies that dealer-permissioned third-party access to the dealer’s own data is “illegal” or “hostile.” Authenticom admits that it retrieves dealer data on the dealer’s DMS. Authenticom further admits that it continues to work with dealers to retrieve data from their DMSs, using login credential created and issued by the dealers. Authenticom denies the remaining allegations in Paragraph 94.

95. Unless Authenticom is permanently enjoined from raiding CDK’s DMS through the unlawful and unauthorized practices set forth above, it will continue to do so in perpetuity. With every security measure that CDK implements, Authenticom will look for what Mr. Cottrell euphemistically calls a “technology solution.” Authenticom’s business model for so-called “data integration” services depends on it. Absent an injunction, CDK will be forced into endless litigation to enforce its fundamental right to exclude unwanted incursions into its DMS.

ANSWER: Paragraph 95 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer is required, Authenticom denies the allegations in Paragraph 95.

**FIRST COUNTERCLAIM FOR RELIEF
(Violations of the Computer Fraud and Abuse Act)**

96. Paragraphs 1-95 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

97. The Computer Fraud and Abuse Act (“CFAA”) provides that “[w]hoever ... intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer,” is subject both to criminal and civil liability. 18 U.S.C. § 1030(a)(2)(C); *see also id.* § 1030(c) (criminal penalties); *id.* § 1030(g) (civil damages and injunctive relief). The CFAA provides for a private cause of action for “compensatory damages and injunctive relief or other equitable relief” to anyone who suffers at least \$5,000 in damage or loss in any one-year period “by reason of a violation” of its terms. *Id.* § 1030(g); *see id.* § 1030(c)(4)(A)(i)(I).

ANSWER: Paragraph 97 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 97 of the Counterclaims.

98. CDK’s DMS is a “computer” within the meaning of the CFAA, which defines that term to include “any data storage facility or communications facility directly related to or operating in conjunction with [a computing] device.” *Id.* § 1030(e)(1). CDK’s DMS also relies on the operation of one or more computing devices in its operations. The DMS itself, and the computing devices by which it operates, are “protected computers” within the meaning of the CFAA because they are connected to the internet and thus are used in and affect interstate and foreign commerce and communications. *See id.* § 1030(e)(2)(B).

ANSWER: Paragraph 98 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 98 of the Counterclaims.

99. Authenticom has repeatedly and intentionally accessed the CDK DMS without CDK’s authorization. CDK’s dealer contracts prohibit dealers from granting Authenticom and other third parties access to the CDK DMS without CDK’s consent. At all relevant times, Authenticom was aware of this access restriction and chose to ignore it.

ANSWER: Paragraph 99 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 99 of the Counterclaims.

100. CDK has informed Authenticom that its access to CDK's DMS is unauthorized and demanded that it cease its hostile access, but Authenticom has refused to do so.

ANSWER: Paragraph 100 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 100 of the Counterclaims.

101. Authenticom accesses CDK's DMS every day and obtains information, including but not limited to the information that Authenticom provides to vendors as part of the "data integration" services it sells them.

ANSWER: Paragraph 101 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the allegations in Paragraph 101 of the Counterclaims.

102. Authenticom's violations of the CFAA have caused substantial damages to CDK. These damages and losses include the costs of investigating and responding to Authenticom's unlawful actions; the costs of restoring the DMS and the data it contains to their condition prior to Authenticom's unlawful actions; and all revenue lost, costs incurred, and other consequential damages incurred because of disruption of service caused by Authenticom's unauthorized access.

ANSWER: Paragraph 102 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 102 of the Counterclaims.

103. Authenticom will continue to violate the CFAA if not enjoined by this Court. Moreover, Authenticom's unauthorized access to the CDK DMS dramatically increases the risk that CDK will suffer a security breach and widespread data corruption issues and degrades the performance of its DMS, all of which constitute an irreparable harm.

ANSWER: Paragraph 103 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 103 of the Counterclaims.

104. CDK is also entitled to equitable relief in the form of restitution for the benefits that Authenticom accrued and/or disgorgement of its profits.

ANSWER: Paragraph 104 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 104 of the Counterclaims.

**SECOND COUNTERCLAIM FOR RELIEF
(Violations of the Digital Millennium Copyright Act)**

105. Paragraphs 1-104 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

106. The Digital Millennium Copyright Act, 17 U.S.C. § 1201 (“DMCA”), prohibits three types of conduct:

- a) “[C]ircumvent[ing] a technological measure that effectively controls access to a work protected under this title” (*Id.* § 1201(a)(1)(A));
- b) “[M]anufactur[ing], import[ing], offer[ing] to the public, provid[ing], or otherwise traffic[king] in any technology, product, service, device, component, or part thereof, that—(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or (C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in

circumventing a technological measure that effectively controls access to a work protected under this title” (*Id.* § 1201(a)(2)); and

- c) “[M]anufactur[ing], import[ing], offer[ing] to the public, provid[ing], or otherwise traffic[king] in any technology, product, service, device, component, or part thereof, that—(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or (C) is marketed by that person or another acting in concert with that person with that person’s knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.” *Id.* § 1201(b)(1).

ANSWER: Paragraph 106 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 106 of the Counterclaims.

107. CDK uses several technological measures to control access to and prevent copying of the CDK DMS software program. These technological measures include: requiring dealer employees to log on with passwords; text prompts asking a user to certify that he or she is an authorized dealer employee; and disabling of dealer credentials that CDK finds have been used for automated access by Authenticom or other third parties. These measures effectively control access to the DMS software program, in that the program cannot be run, and its original, expressive elements cannot be displayed or copied, unless these measures have been navigated. These access control measures were effective in preventing Authenticom from accessing the CDK DMS before Authenticom circumvented them.

ANSWER: Paragraph 107 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 107 of the Counterclaims.

108. Authenticom has repeatedly circumvented CDK’s access control measures in order to access the CDK DMS, extract data from it, and push data back into it. Authenticom has wrongfully obtained login credentials, in violation of contractual requirements that such credentials be given to authorized dealer employees only. It has circumvented, or given outright false answers to, multiple challenge prompts. And after CDK disabled login credentials that had been improperly used for automated DMS access by third parties, Authenticom worked to evade this form of blocking by having new credentials created on its behalf and/or by restoring disabled credentials—including by automated means. This conduct constitutes circumvention of

technological measures that effectively controlled access to CDK's DMS, in violation of Section 1201(a)(1)(A).

ANSWER: Paragraph 108 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 108 of the Counterclaims.

109. Authenticom has also violated Section 1201(a)(2) and 1201(b)(1) by offering its data extraction services to the public. Aspects of Authenticom's technology and service offerings are primarily designed or produced for use in circumventing the access controls on CDK's DMS, because portions of the product are designed and produced primarily for the purpose of bypassing CDK's password controls, text prompts, and credential disabling. Authenticom has therefore violated Sections 1201(a)(2) and 1201(b)(1).

ANSWER: Paragraph 109 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 109 of the Counterclaims.

110. Authenticom has also violated Section 1201(a)(2) and 1201(b)(1) by offering a service to the public, a part of which has limited commercially significant purpose or use other than circumventing the access and anticopying controls on the CDK DMS.

ANSWER: Paragraph 110 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 110 of the Counterclaims.

111. Authenticom has also violated Section 1201(a)(2) and 1201(b)(1) by offering to a service to the public, a part of which Authenticom markets for use in circumventing the access controls on the CDK DMS terminal.

ANSWER: Paragraph 111 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 111 of the Counterclaims.

112. Under 17 U.S.C. § 1203, CDK is entitled to either actual damages and any additional profits from Authenticom's violations of the DMCA or statutory damages, at CDK's election. CDK is also entitled to injunctive relief under 17 U.S.C. § 1203(b)(1). Authenticom will continue to violate the DMCA if not enjoined by this Court. Moreover, Authenticom's unauthorized access to the CDK DMS dramatically increases the risk that CDK will suffer a

security breach and widespread data corruption issues and degrades the performance of its DMS, all of which constitute an irreparable harm.

ANSWER: Paragraph 112 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 112 of the Counterclaims.

**THIRD COUNTERCLAIM FOR RELIEF
(Violations of the Defend Trade Secrets Act)**

113. Paragraphs 1-112 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

114. The Defend Trade Secrets Act provides the owner of a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce a cause of action against a party that has misappropriated that trade secret. 18 U.S.C. § 1836(b).

ANSWER: Paragraph 114 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 114 of the Counterclaims.

115. CDK's DMS contains numerous CDK-proprietary trade secrets, including CDK-created forms, accounting rules, tax tables, and proprietary tools and data compilations. These trade secrets relate to CDK's DMS services, which are licensed and/or sold in interstate and foreign commerce. Authenticom misappropriated these trade secrets by repeatedly gaining access to CDK's DMS through improper means, including by using login credentials it was not authorized to use, evading or bypassing technological measures intended to prevent automated third party access, and wrongful creation of login credentials or reinstatement of disabled credentials. Authenticom knew or had reason to know that its unauthorized access to and copying of information from the CDK DMS was improper.

ANSWER: Paragraph 115 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 115 of the Counterclaims.

116. Authenticom has been unjustly enriched by its misappropriation of CDK's trade secrets, and CDK is entitled to disgorgement of those profits. In the alternative, CDK is entitled to payment of a reasonable royalty for Authenticom's acquisition, use, and possession of CDK's trade secrets.

ANSWER: Paragraph 116 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 116 of the Counterclaims.

117. Authenticom's misappropriation of CDK's trade secrets will continue unless enjoined by this Court, causing CDK irreparable harm.

ANSWER: Paragraph 117 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 117 of the Counterclaims.

**FOURTH COUNTERCLAIM FOR RELIEF
(Violations of the Wisconsin Computer Crimes Act)**

118. Paragraphs 1-117 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

119. The Wisconsin Computer Crimes Act ("WCCA") prohibits "willfully, knowingly and without authorization" accessing, taking possession of, or copying "computer programs or supporting documentation." Wis. Stat. § 943.70(2)(a).

ANSWER: Paragraph 119 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 119 of the Counterclaims.

120. The WCCA provides that “[a]ny aggrieved party may sue for injunctive relief ... to compel compliance with this section.” *Id.* § 943.70(5).

ANSWER: Paragraph 120 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 120 of the Counterclaims.

121. CDK’s DMS is a “computer program” within the meaning of the WCCA, which defines that term to include not just computing devices themselves, but also “all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer in a computer system or computer network.” *Id.* § 943.70(1)(am).

ANSWER: Paragraph 121 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 121 of the Counterclaims.

122. Authenticom has willfully and repeatedly accessed, taken possession of, and/or copied CDK’s DMS and programs within the DMS. At all relevant times, Authenticom knew that dealers are forbidden by their contracts with CDK from giving Authenticom or other data integrators access to the DMS without CDK’s consent.

ANSWER: Paragraph 122 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 122 of the Counterclaims.

123. CDK is an “aggrieved party” within the meaning of the WCCA because it is the owner and operator of the CDK DMS that Authenticom has illegally accessed; because Authenticom has intentionally induced and caused CDK’s dealer customers to violate the terms of their contracts with CDK; because Authenticom has unjustly enriched itself at CDK’s expense; and because Authenticom has caused CDK various other damages and losses as set forth in these Counterclaims.

ANSWER: Paragraph 123 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 123 of the Counterclaims.

124. Authenticom will continue to violate the WCCA unless enjoined by this Court. Moreover, Authenticom's unauthorized access to the CDK DMS dramatically increases the risk that CDK will suffer a security breach and widespread data corruption issues and degrades the performance of its DMS, all of which constitute an irreparable harm.

ANSWER: Paragraph 124 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 124 of the Counterclaims.

**FIFTH COUNTERCLAIM FOR RELIEF
(Misappropriation of Trade Secrets)**

125. Paragraphs 1-124 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

126. The Wisconsin Uniform Trade Secrets Act, Wis. Stat. § 134.90, prohibits misappropriation of trade secrets.

ANSWER: Paragraph 126 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 126 of the Counterclaims.

127. CDK's DMS contains numerous proprietary CDK trade secrets, including forms, accounting rules, tax tables, and proprietary tools and data compilations.

ANSWER: Paragraph 127 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 127 of the Counterclaims.

128. The CDK trade secrets stored on the CDK DMS derive independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, such as other DMS providers, application providers, or third-party data extractors like Authenticom.

ANSWER: Paragraph 128 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 128 of the Counterclaims.

129. CDK makes efforts to maintain the secrecy of these trade secrets that are reasonable under the circumstances. CDK secures its DMS with password control and places strict contractual limitations on who may be granted password access to the DMS. CDK also uses automated prompts and other measures to prevent DMS access by automated screen-scraping systems such as Authenticom's. CDK does not generally share these trade secrets except in narrow circumstances and subject to strict constraints on further disclosure.

ANSWER: Paragraph 129 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 129 of the Counterclaims.

130. Authenticom misappropriated these trade secrets by improperly acquiring login credentials from CDK's dealer customers, using those credentials to access the CDK DMS without authorization, circumventing multiple access controls, and copying data. The means by which Authenticom acquired these trade secrets was clearly improper, in that it violated both federal and state laws and the terms of CDK's dealer contract. Authenticom thus knew or had reason to know that these means were improper.

ANSWER: Paragraph 130 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 130 of the Counterclaims.

131. Authenticom has been unjustly enriched by its misappropriation of CDK's trade secrets, and CDK is entitled to disgorgement of those profits.

ANSWER: Paragraph 131 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 131 of the Counterclaims.

132. In the alternative, CDK is entitled to payment of a reasonable royalty for Authenticom's acquisition, use, and possession of CDK's trade secrets.

ANSWER: Paragraph 132 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 132 of the Counterclaims.

133. Authenticom's misappropriation of CDK's trade secrets will continue unless enjoined by this Court, causing CDK irreparable harm.

ANSWER: Paragraph 133 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 133 of the Counterclaims.

**SIXTH COUNTERCLAIM FOR RELIEF
(Violations of the California Comprehensive Computer Data Access and Fraud Act)**

134. Paragraphs 1-133 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

135. The California Comprehensive Computer Data Access and Fraud Act ("CCCDFA") provides for criminal and civil liability against "any person" who, among other specified misconduct:

- a) "[k]nowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data";
- b) "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network";

- c) “[k]nowingly and without permission uses or causes to be used computer services”;
- d) “[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network”;
- e) “[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section”; and
- f) “[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.” Cal. Penal Code § 502(c)(1)-(4), (6)-(7).

ANSWER: Paragraph 135 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 135 of the Counterclaims.

136. The CCCDAFA further provides that, “[i]n addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of” any of these violations “may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief.” *Id.* § 502(e)(1).

ANSWER: Paragraph 136 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 136 of the Counterclaims.

137. CDK’s DMS constitutes and/or comprises a “computer network[,],” “computer system[,],” and “computer program[] or software,” and CDK provides “computer services” to its dealer customers and authorized vendors, including in California, within the meaning of the CCCDAFA. A substantial portion of CDK’s networks and systems are located in California.

ANSWER: Paragraph 137 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 137 of the Counterclaims.

138. As set forth above, Authenticom has repeatedly and knowingly accessed the CDK DMS without CDK’s permission, including in California, and has knowingly and without permission engaged in numerous other actions prohibited by the CCCDAFA. Authenticom has

knowingly and without permission accessed and used CDK's DMS to wrongfully obtain data within the DMS and provide it to third-party vendors; knowingly and without permission attempted to deceive and defraud CDK by tricking the DMS into believing that Authenticom was an authorized dealer employee logging into his or her own account, for the purpose of taking data from the DMS and providing it to third-party vendors; knowingly and without permission used a variety of computer services provided by the CDK DMS; and knowingly and without permission accessing, causing to be accessed, and assisting others in accessing the CDK DMS.

ANSWER: Paragraph 138 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 138 of the Counterclaims.

139. A substantial portion of these illegal activities either took place in California or were targeted at computers, computer systems, and computer networks located there; were undertaken at the behest of and in coordination with dealers and vendors located in California; and involved confidential data of California residents.

ANSWER: Paragraph 139 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 139 of the Counterclaims.

140. The CCCDAFA violations identified above have caused damages to CDK, including the costs of investigating and responding to Authenticom's unlawful actions; the costs of restoring the CDK DMS and the data it contains to their condition prior to Authenticom's unlawful actions; and all revenue lost, costs incurred, and other consequential damages incurred because of disruption of service caused by Authenticom's unauthorized access.

ANSWER: Paragraph 140 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 140 of the Counterclaims.

141. Authenticom's violations of the CCCDAFA will continue if not enjoined by this Court. Moreover, Authenticom's unauthorized access to the CDK DMS dramatically increases the risk that CDK will suffer a security breach and widespread data corruption issues and degrades the performance of its DMS, all of which constitute an irreparable harm.

ANSWER: Paragraph 141 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 141 of the Counterclaims.

142. CDK is also entitled to equitable restitution for the benefits that Authenticom accrued and/or disgorgement of its profits.

ANSWER: Paragraph 142 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 142 of the Counterclaims.

**SEVENTH COUNTERCLAIM FOR RELIEF
(California Unfair Competition Law)**

143. Paragraphs 1-142 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

144. The California Unfair Competition Law prohibits “any unlawful, unfair or fraudulent business act or practice” Cal. Bus. & Prof. Code § 17200.

ANSWER: Paragraph 144 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 144 of the Counterclaims.

145. Authenticom’s business acts and practices, including but not limited to its misappropriation and unauthorized use of DMS login credentials; circumvention of access and anticopying controls; and provision to the public of a service that facilitates circumvention of access and anticopying controls are unlawful under, *inter alia*, the CFAA; the WCCA; the CCCDFA; and the DMCA.

ANSWER: Paragraph 145 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 145 of the Counterclaims.

146. Authenticom's business acts and practices, including but not limited to its misappropriation and unauthorized use of DMS login credentials and inducement of CDK's dealer customers to breach their contracts with CDK are also unfair practices under the UCL. It is unfair and inequitable for Authenticom to violate CDK's legitimate restrictions on DMS access in order to free-ride on CDK's proprietary system and technology for its own profit.

ANSWER: Paragraph 146 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 146 of the Counterclaims.

147. A substantial portion of Authenticom's unlawful and unfair activities occurred in California, where many CDK dealer customers are located.

ANSWER: Paragraph 147 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 147 of the Counterclaims.

148. CDK has suffered economic injury as a result of Authenticom's unlawful and unfair business practices. CDK has had to devote substantial resources to monitoring and remediating any harmful effects of Authenticom's unauthorized DMS access and to preventing such unauthorized access in the future. CDK has also been denied any compensation for Authenticom's access to the CDK DMS.

ANSWER: Paragraph 148 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 148 of the Counterclaims.

149. CDK is entitled to restitution for the benefits that Authenticom accrued and/or disgorgement of its profits.

ANSWER: Paragraph 149 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 149 of the Counterclaims.

150. Authenticom's unlawful business practices will continue if not enjoined by this Court. Moreover, Authenticom's unauthorized access to the CDK DMS dramatically increases the risk that CDK will suffer a security breach and widespread data corruption issues and degrades the performance of its DMS, all of which constitute an irreparable harm.

ANSWER: Paragraph 150 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 150 of the Counterclaims.

**EIGHTH COUNTERCLAIM FOR RELIEF
(Tortious Interference With Contract)**

151. Paragraphs 1-150 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

152. CDK enters into a valid and binding written contract with each of its dealer customers, referred to as the Master Services Agreement.

ANSWER: Paragraph 152 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 152 of the Counterclaims.

153. CDK's Master Services Agreement prohibits dealers from allowing third-party data extractors like Authenticom to access the CDK DMS without CDK's consent. Authenticom was aware of these contractual restrictions and has encouraged dealers to violate them.

ANSWER: Paragraph 153 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 153 of the Counterclaims.

154. At all relevant times, Authenticom knew that dealers who provided it with login credentials for the CDK DMS for purposes of accessing the DMS and its constituent programs, extracting data, providing the data to vendors, and writing data back into the DMS were breaching their contracts with CDK. Authenticom intentionally interfered with those contractual relationships by selling data integration services to dealers.

ANSWER: Paragraph 154 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 154 of the Counterclaims.

155. Authenticom's interference with CDK's dealer contracts was the direct and proximate cause of damages to CDK. As a result of Authenticom's interference and the breaches of the dealer contracts, CDK has had to devote substantial resources to monitoring and remediating any harmful effects of Authenticom's unauthorized DMS access and to preventing such unauthorized access in the future. CDK has also been denied any compensation for Authenticom's access to the CDK DMS. CDK was also damaged in that Authenticom enjoyed free access to the CDK DMS for which it otherwise would have had to pay.

ANSWER: Paragraph 155 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 155 of the Counterclaims.

156. Authenticom was neither justified nor privileged to interfere with CDK's contractual relationships with its dealers in this way. Authenticom knew that the terms of CDK's dealer contracts forbade it from accessing the CDK DMS without CDK's authorization but deliberately pursued a business model that violated and undermined that restriction on access in order to profit off of CDK's substantial investments in its DMS technology.

ANSWER: Paragraph 156 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 156 of the Counterclaims.

157. Authenticom's tortious interference with CDK's dealer contracts will continue into the future if not enjoined by this Court. Moreover, Authenticom's unauthorized access to the CDK DMS dramatically increases the risk that CDK will suffer a security breach and widespread

data corruption issues and degrades the performance of its DMS, all of which constitute an irreparable harm.

ANSWER: Paragraph 157 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 157 of the Counterclaims.

**NINTH COUNTERCLAIM FOR RELIEF
(Trespass to Chattels)**

158. Paragraphs 1-157 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

159. Authenticom's repeated circumvention of the access controls on the CDK DMS, and its repeated access thereto, constitute trespass to chattels.

ANSWER: Paragraph 159 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 159 of the Counterclaims.

160. At all relevant times, Authenticom knew that its access to the CDK DMS was not authorized, but it intentionally and repeatedly accessed the DMS despite CDK's opposition.

ANSWER: Paragraph 160 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 160 of the Counterclaims.

161. Authenticom's access to, extraction of data from, and writing data back into the CDK DMS impaired the condition, quality, and value of the DMS by slowing its performance, impeding its operations, subjecting it to data corruption and system integrity issues, and exposing it to heightened security threats.

ANSWER: Paragraph 161 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 161 of the Counterclaims.

162. Authenticom's trespasses have directly and proximately harmed CDK by diminishing the functionality, efficiency, and usefulness of its DMS.

ANSWER: Paragraph 162 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 162 of the Counterclaims.

TENTH COUNTERCLAIM FOR RELIEF (Conversion)

163. Paragraphs 1-162 above are incorporated herein by reference.

ANSWER: Defendant's claims and theories premised on Plaintiff's purported Conversion were dismissed by the Court and have not been repled. Dkt. 506. As a result, no response is required. To the extent a response is required, Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

164. Every time Authenticom accesses the CDK DMS and the DMS database software program, it intentionally controls servers owned by CDK, which execute the search queries submitted by Authenticom and return the data requested.

ANSWER: Defendant's claims and theories premised on Plaintiff's purported Conversion were dismissed by the Court and have not been repled. Dkt. 506. As a result, no response is required. Paragraph 164 of the Counterclaims states legal conclusions to which no answer is

required. To the extent an answer may be required, Authenticom denies the allegations in Paragraph 164 of the Counterclaims.

165. CDK does not consent and has never consented to Authenticom's exercise of control over its server systems.

ANSWER: Defendant's claims and theories premised on Plaintiff's purported Conversion were dismissed by the Court and have not been repled. Dkt. 506. As a result, no response is required. Paragraph 165 of the Counterclaims states legal conclusions to which no answer is required. To the extent an answer may be required, Authenticom denies the allegations in Paragraph 165 of the Counterclaims.

166. Authenticom's repeated access to the CDK DMS seriously interfered with CDK's possessory rights in its server systems by reducing the efficiency and efficacy of the server systems. This interference has been a direct and proximate cause of harm and damages to CDK.

ANSWER: Defendant's claims and theories premised on Plaintiff's purported Conversion were dismissed by the Court and have not been repled. Dkt. 506. As a result, no response is required. Paragraph 166 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 166 of the Counterclaims.

**ELEVENTH COUNTERCLAIM FOR RELIEF
(Unjust Enrichment)**

167. Paragraphs 1-166 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

168. Every time Authenticom accesses the CDK DMS without authorization, the DMS automatically confers several benefits upon Authenticom.

ANSWER: Paragraph 168 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 168 of the Counterclaims.

169. First, Authenticom is able to extract data from the CDK DMS and write data back into it, which enables it to provide data extraction and writeback services to vendors and to be paid by vendors for those services.

ANSWER: Paragraph 169 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 169 of the Counterclaims.

170. Second, Authenticom enjoys free access to the CDK DMS, which is a benefit for which it would otherwise have to pay (through CDK's 3PA program).

ANSWER: Paragraph 170 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 170 of the Counterclaims.

171. Authenticom knows and appreciates that CDK is conferring benefits upon Authenticom when Authenticom accesses CDK's DMS. Authenticom recognizes such benefits when, among other things, it makes representations that, if CDK is permitted to block it from accessing the CDK DMS, it will go out of business. *See, e.g.,* Compl. ¶ 233.

ANSWER: Paragraph 171 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 171 of the Counterclaims.

172. Authenticom has accepted and retained these ill-gotten benefits under such circumstances that it would be inequitable to allow it to retain the benefits without paying for the value thereof. Authenticom's unauthorized access is unlawful and violates the terms of CDK's dealer contracts. Authenticom also knows that CDK does not want Authenticom to access the CDK DMS but has persisted in doing so for its own purposes and its own profit. It would be inequitable in these circumstances to allow Authenticom to retain the benefits of its unauthorized access without paying compensation to CDK.

ANSWER: Paragraph 172 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 172 of the Counterclaims.

**TWELFTH COUNTERCLAIM FOR RELIEF
(Fraud)**

173. Paragraphs 1-172 above are incorporated herein by reference.

ANSWER: Authenticom incorporates, as if fully set forth herein, its answers to the preceding paragraphs of the Counterclaims.

174. In the course of accessing the CDK DMS without authorization, Authenticom has frequently and repeatedly represented to CDK that it is a human employee of a CDK dealer customer who is authorized to access the DMS. That representation occurs whenever Authenticom uses login credentials provided by dealers, which are only intended permitted to be used by authorized dealership employees. Authenticom has also responded “YES” to text prompts during the DMS login process expressly asking whether it is an authorized dealership employee, and has entered CAPTCHA responses when prompted to “[e]nter the following text to confirm you are an authorized dealer employee.”

ANSWER: Paragraph 174 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 174 of the Counterclaims.

175. Those representations are false. Authenticom is not a dealer employee and is forbidden under CDK’s dealer contracts from accessing the CDK DMS. Authenticom knows these facts and thus knows that its representations to CDK are untrue.

ANSWER: Paragraph 175 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 175 of the Counterclaims.

176. CDK frequently believes Authenticom’s false misrepresentations to be true and relies on them by allowing Authenticom to access the CDK DMS. CDK’s technological measures have not always been effective to detect Authenticom’s unauthorized access; even today, they are

sometimes unable to determine that Authenticom is not an authorized employee of a CDK dealer customer. If CDK always knew when Authenticom was attempting to access its system without authorization, it would prevent Authenticom from ever doing so.

ANSWER: Paragraph 176 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 176 of the Counterclaims.

177. Authenticom's fraudulent misrepresentations are the direct and proximate cause of harm and damages to CDK. As a result of Authenticom's interference and the breaches of the dealer contracts, CDK has had to devote substantial resources to monitoring and remediating any harmful effects of Authenticom's unauthorized DMS access and to preventing such unauthorized access in the future. CDK has also been denied any compensation for Authenticom's access to the CDK DMS. CDK was also damaged in that Authenticom enjoyed free access to the CDK DMS for which it otherwise would have had to pay.

ANSWER: Paragraph 177 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. To the extent that an answer may be required, Authenticom denies the remaining allegations in Paragraph 177 of the Counterclaims.

178. Authenticom's fraud will continue if not enjoined by this Court. Among other things, Authenticom's unauthorized access to the CDK DMS dramatically increases the risk that CDK will suffer a security breach and widespread data corruption issues and degrades the performance of its DMS, all of which would constitute an irreparable harm because money damages would not compensate for the reputational injury that CDK would experience from such a breach.

ANSWER: Paragraph 178 of the Counterclaims states legal conclusions to which no answer is required. To the extent that an answer may be required, Authenticom denies that CDK or any other individual or entity has suffered, or is made more likely to suffer, any injury as a result of any action or conduct of Authenticom and therefore denies that CDK is entitled to the relief it seeks. Authenticom denies the remaining allegations in Paragraph 178 of the Counterclaims.

JURY DEMAND

In accordance with Federal Rule of Civil Procedure 38(b), CDK demands a trial by jury on all issues so triable.

ANSWER: To the extent that an answer may be required to the Jury Demand at the end of CDK's Counterclaims, Authenticom denies each and every allegation therein.

PRAYER FOR RELIEF

ANSWER: To the extent that an answer may be required to the Prayer for relief at the end of the Counterclaims, Authenticom denies each and every allegation contained therein and denies that CDK is entitled to the relief it seeks.

* * * * *

DENIAL

Authenticom denies each and every allegation of the Counterclaims not specifically admitted above.

AFFIRMATIVE AND ADDITIONAL DEFENSES

Without assuming any burden of proof that it would not otherwise bear, Authenticom also asserts the following affirmative and additional defenses:

First Defense

The Counterclaims fail to state a claim upon which relief may be granted.

Second Defense

As detailed in Authenticom's complaint, CDK's actions and contracts purporting to prohibit Authenticom's business activities are part of an unlawful scheme to eliminate competition. As such, the contractual and legal restrictions alleged herein are void as a matter of law. As a result, CDK has failed to state a cause of action.

Third Defense

CDK's claim is barred, in whole or in part, by the applicable statute of limitations. CDK filed these Counterclaims on June 29, 2018. CDK has not pled any event that would toll any applicable limitations period. As such, the statutory time limitation applicable to some or all of CDK's claims has passed and thus are time-barred.

Fourth Defense

If and to the extent that CDK has been damaged, which Authenticom denies, the amount of damages that CDK alleges to have suffered is too remote or speculative to allow recovery, and it is impossible to ascertain and allocate such alleged damages with reasonable certainty.

Fifth Defense

If and to the extent CDK has been damaged, which Authenticom denies, CDK, by the exercise of reasonable diligence, could have mitigated its damages but did not, and CDK is therefore barred from recovery. Alternatively, any damages sustained by CDK, which Authenticom denies, must be reduced by the amount that such damages would have been reduced had CDK exercised reasonable diligence in mitigating its damages.

Sixth Defense

CDK's claims are barred, in whole or in part, because to the extent CDK suffered any injury or incurred any damages as alleged in the Counterclaims, which Authenticom denies, any such injury or damage was caused and brought about by the acts, conduct or omissions of individuals or entities other than Authenticom and, as such, any recovery herein should be precluded or diminished in proportion to the amount of fault attributable to such other individuals or entities.

Seventh Defense

CDK's claims are barred by the doctrine of unclean hands. The unclean hands doctrine bars CDK from bringing these claims to allege that Authenticom engaged in unlawful activity based on the manner in which Authenticom has organized its corporate infrastructure, facilities, personnel, job responsibilities, and computer systems, because Authenticom is informed and believes that CDK have themselves made similar decisions and engage in similar practices to those alleged of Authenticom, including with regard to independent data integration services, both on its own behalf and by and through its subsidiaries and affiliates. The unclean hands doctrine demands that a plaintiff act fairly in the matter for which it seeks a remedy. The plaintiff must come into court with clean hands, and keep them clean, or it will be denied relief, regardless of the merits of its claim. The defense applies to bar legal and equitable claims, and need not involve criminal or tortious activity – simply conduct that violates conscience, good faith, and equitable standards of conduct. To the extent CDK seeks to contend that Authenticom engaged in unlawful activity by allegedly performing the same or similar acts as CDK, within the same nexus of common customers and common sources of data or classes of software, its claims are barred because such conduct infects its claims and renders pursuing this action inequitable.

Eighth Defense

To the extent lack of authorization for access is deemed an affirmative defense rather than an element on which CDK bears the burden of proof (and Authenticom contends that the latter applies), CDK is barred from claiming violations of any statute or source of law because Authenticom's access was authorized.

Ninth Defense

CDK's claims are barred by the doctrine of acquiescence.

Tenth Defense

CDK's claims are barred by the doctrines of laches, waiver, and estoppel.

Eleventh Defense

To the extent that ready ascertainability is deemed an affirmative defense rather than an element on which CDK bears the burden of proof (and Authenticom contends that the latter applies), CDK is barred from claiming trade secret misappropriation as to any items of information that were readily ascertainable within the meaning of that defense at the time of the alleged misappropriation.

Twelfth Defense

To the extent that independent derivation is deemed an affirmative defense rather than an element on which CDK bears the burden of proof (and Authenticom contends that the latter applies), CDK is barred from claiming trade secret misappropriation as to any items of information that it independently derived within the meaning of that defense.

Thirteenth Defense

The privilege of competition and other privileges available under state law bar CDK from pursuing its claims for relief.

Fourteenth Defense

The doctrine of implied license bars CDK from pursuing their claims for relief.

Fifteenth Defense

CDK's claims are barred by the doctrines of copyright misuse and copyright abuse.

Sixteenth Defense

CDK's claims are barred because Authenticom's conduct constituted fair use.

Sixteenth Defense

CDK's claims are barred, in whole or in part, because CDK has not suffered any legally cognizable injury, including because CDK has not suffered an injury-in-fact and its alleged injuries are too speculative, indirect and remote from the alleged conduct, and cannot be ascertained and apportioned.

Seventeenth Defense

CDK's claims are barred, in whole or in part, because to the extent CDK suffered any injury or incurred any damages as alleged, which Authenticom denies, Authenticom's alleged conduct was not the actual or proximate cause of any injury or damage to CDK.

Eighteenth Defense

CDK's claims are barred, in whole or in part, because any recovery would result in unjust enrichment to CDK.

Nineteenth Defense

CDK is barred from recovering because its acts are in violation of public policy

* * * * *

Authenticom adopts by reference any applicable defense pled by any other counterclaim-defendant not expressly set forth herein. In addition, Authenticom has insufficient knowledge or information upon which to form a basis as to whether it may have additional, as yet unstated, separate defenses available. Authenticom reserves the right to amend this Answer to add, supplement or modify defenses based upon legal theories that may be or will be divulged, through discovery, or through further factual or legal analysis of CDK's allegations, contentions and positions in this litigation.

JURY DEMAND

Pursuant to Federal Rules of Civil Procedure, Rule 38(b), Authenticom hereby demands trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Authenticom requests that CDK's Counterclaims be dismissed with prejudice, that the Court find that CDK is not entitled to any judgment or relief, that the Court enter judgment in favor of Authenticom, and that the Court award Authenticom its attorneys' fees, costs and expenses, pre-judgment interest, and such other and further relief as the Court deems just and proper.

Dated: February 15, 2019

Respectfully submitted,

/s/ Derek T. Ho

Derek T. Ho

**KELLOGG, HANSEN, TODD,
FIGEL & FREDERICK, P.L.L.C.**

1615 M Street, NW, Suite 400

Washington, D.C. 20036

(202) 326-7900

dho@kellogghansen.com

Counsel for Plaintiff Authenticom, Inc.

CERTIFICATE OF SERVICE

I, Derek T. Ho, an attorney, hereby certify that on February 25, 2019, I caused a true and correct copy of the foregoing **AUTHENTICOM, INC.'S PUBLIC-REDACTED ANSWER AND AFFIRMATIVE AND OTHER DEFENSES TO DEFENDANT CDK GLOBAL, LLC'S COUNTERCLAIMS** to be filed electronically via the court's CM/ECF system. Notice of this filing will be sent by email to all counsel of record by operation of the court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing.

/s/ Derek T. Ho

Derek T. Ho

**KELLOGG, HANSEN, TODD,
FIGEL & FREDERICK, P.L.L.C.**

1615 M Street, NW, Suite 400

Washington, D.C. 20036

(202) 326-7900

dho@kellogghansen.com